UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/626,420	07/24/2003	Sheueling Chang Shantz	6000-32301	9856

58467   7590   06/26/2009
MHKKG/SUN
P.O. BOX 398
AUSTIN, TX 78767

EXAMINER
JOHNSON, CARLTON

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
06/26/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patent_docketing@intprop.com
ptomhkkg@gmail.com

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _____ .
2a) ☒ This action is **FINAL**.   2b) ☐ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1-65</u> is/are pending in the application.
   4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) <u>1-65</u> is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a) ☐ All   b) ☐ Some * c) ☐ None of:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
    3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date <u>3-11-2009</u>.
4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____ .

DETAILED ACTION

1.   This action is responding to application amendments filed on 3-10-2009.

2.   Claims **1 - 65** are pending. Claims **1, 18, 43, 50, 57, 61, 64, 65** are independent.
This application was filed on 7-24-2003.

Response to Arguments

3.   Applicant's arguments have been fully considered but were not persuasive.

3.1   Applicant argues that the referenced prior art does not disclose, *"a single*
arithmetic operation" ; *"adding a third number to generate a result that represents the*
first number multiplied by the second number summed with the partial result and the
third number". *(Remarks Page 7)*

Applicant's claimed invention is a sequence of arithmetic process steps
(multiplication, addition, subtraction) performed and designated at completion as a
single arithmetic instruction.   Chen prior art discloses the same arithmetic process
steps (multiple, addition, subtraction).   In addition, Chen prior art discloses the concept
of feedback whereby a circuit using feedback is defined as: *"the transfer of part of the*
output of an active circuit or device back to the input".   The concept and usage of
feedback enables the processing of a sequence of arithmetic process steps as a single
arithmetic operation or instruction.   In feedback, the output of one arithmetic process
step is input to a next arithmetic process step in a sequence of arithmetic processing

steps. The completion of the set of multiple processing steps results in the completion of a single arithmetic complex operation or instruction.

This claim limitation indicates a sequence of arithmetic process steps resulting in a completed arithmetic operation. The concept of feedback enables a sequence of arithmetic process steps such as multiplication and addition operations to be performed. The concept of feedback allows the output of a process step to be used as input for a next process step. The single arithmetic operation or instruction would be the completion of the set of arithmetic processing steps.

The Examiner is unclear why with the usage of feedback, as used by Chen prior art in the operation of arithmetic processing steps resulting in the completion of a single arithmetic operation or instruction, the claimed invention is not disclosed. The cited prior art indicates each specific arithmetic process step such as multiplication, subtraction, and addition that is performed by the claimed invention. With the usage of feedback the precise arithmetic instruction consisting of the specified required sequence of arithmetic processing steps can be achieved.

3.2   Applicant argues that, "Bushan teaches the opposite of storing a result of one instruction for use in a subsequent computation". (Remarks Page 5)

Bushan prior art discloses that if a current instruction requires the result from a previous instruction. The result can be supplied. This disclosure indicates that the results of one instruction are saved and used as input or as an operand for a next

instruction. There is an additional option where the result may be bypassed. But, the

result may also be used.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art
> are such that the subject matter as a whole would have been obvious at the time the invention was made
> to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be
> negatived by the manner in which the invention was made.

5.   Claims **1, 2, 4, 5, 13 - 16, 18, 19, 21 - 23, 30, 33 - 44, 49 - 51, 56 - 65** are

rejected under 35 U.S.C. 103 (a) as being unpatentable over **Chen et al.** (US Patent

No. **6,763,365**) in view of **Bhushan et al.** (US PGPUB No. **20020174157**).

With Regards to Claim 1, Chen discloses a method implemented in a device

supporting a cryptography application (see Chen col. 6, lines 23-25: arithmetic

operations to support acceleration of cryptographic functions), the method comprising:

in response to executing a single arithmetic instruction, multiplying a first number by a

second number; and adding implicitly a partial result from an executed single arithmetic

instruction to generate a result that represents the first number multiplied by the second

number summed with the partial result, wherein the partial result comprises a high order

portion of a result of the previously executed single arithmetic instruction (see Chen col.

11, lines 34-40: feedback; first using circuit; then using circuit again with register

provided with output from first operational stage; col. 10, lines 13-26: multiple-

accumulate instruction; first addend comes from the rightmost k bits of Z register; bits

are added to the k bits in the rightmost portion of the product A,B); storing at least a

portion of the generated result; and using the stored at least a portion of the generated

result in a subsequent computation in the cryptography application. (see Chen col. 4,

lines 8-11: multiplication and addition are performed by large circuits; col. 10, lines 13-

36; col. 11, lines 34-40: feedback; first using circuit; then using circuit again with

register provided with output from first operational stage (multiplication with feedback))

Bhushan discloses wherein a previously executed single arithmetic instruction to

generate a result. (see Bhushan paragraph [0116], lines 14-20: instruction requires an

operand, a result from a previous instructions, the result may be bypassed under the

direction of bypass routing control)

It would have been obvious to one of ordinary skill in the art to modify Chen for a

previously executed single arithmetic instruction to generate a result as taught by

Bhushan.   One of ordinary skill in the art would have been motivated to employ the

teachings of Bhushan to provide an efficient method for an uncomplicated arithmetic

circuit that is capable of adding or subtracting numbers in redundant from and

comparing a result without requiring propagation of carry signals.   (see Bhushan

paragraph [0062], lines 1-5)

With Regards to Claim 2, Chen discloses the method as recited in claim 1 further

comprising performing the adding of the partial result as part of addition operations

performed for the multiplying of the first and second number. (see Chen col. 10, lines 13-36: addition operation (adder) performed as part of multiplication operation)

With Regards to Claim 4, Chen discloses the method as recited in claim 1, wherein said adding the partial result comprises adding the partial result to a multiplication result of the first and second numbers. (see Chen col. 10, lines 13-36: the lower k bits from multiplier array are supplied to adder; these bits are added to the k bits in the rightmost portion of the product A,B)

With Regards to Claim 5, Chen discloses the method as recited in claim 1, wherein said storing at least a portion of the generated result comprises storing a high order portion of the generated result as a next partial result for use with execution of a subsequent single arithmetic instruction. (see Chen col. 11, lines 34-40: feedback; first using circuit; then using circuit again with register provided with output from first operational stage)

With Regards to Claim 13, Chen discloses the method as recited in claim 1, wherein the single arithmetic instruction is a single multiply-accumulate instruction; wherein the first and second numbers are specified in the single multiply-accumulate instruction as first and second source registers and a low order portion of the result is stored in a destination location specified in the single multiply-accumulate instruction. (see Chen col. 11, lines 34-40: feedback; first using circuit; then using circuit again with register

provided with output from first operational stage; col. 10, lines 23-26: multiple-accumulate instruction; first addend comes from the rightmost k bits of Z register; bits are added to the k bits in the rightmost portion of the product A,B)

With Regards to Claim 14, Chen discloses the method as recited in claim 5 wherein the first and second numbers are n-bit numbers, n being a positive integer and wherein the high order portion of the generated result is an n-bit portion. (see Chen col. 10, lines 13-36: n+1 bits and k (also equal to n+1) bits produces n+1+k bits product; col. 10, lines 37-39: high order n+1 bits)

With Regards to Claim 15, Chen discloses the method as recited in claim 5 further comprising: in response to executing the subsequent single arithmetic instruction, multiplying third and fourth numbers specified by the subsequent single arithmetic instruction and adding implicitly the next partial result to generate a second result that represents the third number multiplied by the fourth number summed with the next partial result. (see Chen col. 10, lines 13-36; col 11, lines 34-40: feedback operations; feedback; first using circuit; then using circuit again with register provided with output from first operational stage)

With Regards to Claim 16, Chen discloses the method as recited in claim 15, further comprising storing the high order portion of the second result to be implicitly added in response to executing another subsequent single arithmetic instruction. (see Chen col.

11, lines 34-40: feedback; first using circuit; then using circuit again with register

provided with output from first operational stage; col. 10, lines 23-26: multiple-

accumulate instruction; first addend comes from the rightmost k bits of Z register; bits

are added to the k bits in the rightmost portion of the product A,B)

With Regards to Claim 18, Chen discloses a method implemented in a device

supporting a cryptography application, the method comprising: in response to executing

a single arithmetic instruction, multiplying a first number by a second number; adding

implicitly a partial result from an executed single arithmetic instruction, wherein the

partial result comprises a high order portion of a result of the previously executed single

arithmetic instruction; adding a third number to generate a result that represents the first

number multiplied by the second number summed with the partial result and the third

number; storing at least a portion of the generated result; and using the stored at least a

portion of the generated result in a subsequent computation in the cryptography

application.   (see Chen col. 4, lines 8-11: multiplication and addition are performed by

large circuits; col. 10, lines 13-36; col. 11, lines 34-40: multiplication with feedback; col.

6, lines 23-25: arithmetic operations to support acceleration of cryptographic functions)

Bhushan discloses wherein a previously executed single arithmetic instruction. (see

Bhushan paragraph [0116], lines 14-20: instruction requires an operand, a result from a

previous instructions, the result may be bypassed under the direction of bypass routing

control)

It would have been obvious to one of ordinary skill in the art to modify Chen for a

previously executed single arithmetic instruction as taught by Bhushan. One of ordinary

skill in the art would have been motivated to employ the teachings of Bhushan in order

to provide an efficient method for an uncomplicated arithmetic circuit that is capable of

adding or subtracting numbers in redundant from and comparing a result without

requiring propagation of carry signals. (see Bhushan paragraph [0062], lines 1-5)

With Regards to Claim 19, Chen discloses the method as recited in claim 18 further

comprising performing the adding of the partial result as part of addition performed for

the multiplying of the first and second number. (see Chen col. 11, lines 34-40: feedback;

first using circuit; then using circuit again with register provided with output from first

operational stage; col. 10, lines 23-26: multiple-accumulate instruction; first addend

comes from the rightmost k bits of Z register; bits are added to the k bits in the rightmost

portion of the product A,B)

With Regards to Claim 21, Chen discloses the method as recited in claim 18 further

comprising performing the adding of the third number as part of the addition performed

for the multiplying of the first and second number. (see Chen col. 11, lines 34-40:

feedback; first using circuit; then using circuit again with register provided with output

from first operational stage; col. 10, lines 23-26: multiple-accumulate instruction; first

addend comes from the rightmost k bits of Z register; bits are added to the k bits in the

rightmost portion of the product A,B)

With Regards to Claim 22, Chen discloses the method as recited in claim 18, wherein

said adding the partial result comprises adding the partial result after generation of a

multiplication result of multiplying the first and second numbers. (see Chen col. 11, lines

34-40: feedback; first using circuit; then using circuit again with register provided with

output from first operational stage; col. 10, lines 23-26: multiple-accumulate instruction;

first addend comes from the rightmost k bits of Z register; bits are added to the k bits in

the rightmost portion of the product A,B)

With Regards to Claim 23, Chen discloses the method as recited in claim 18, wherein

said storing at least a portion of the generated result comprises storing a high order

portion of the generated result as a next partial multiplication result for use with

execution of a subsequent single arithmetic instruction. (see Chen col. 10, lines 32-36:

rightmost k bits from multiplier are supplied back to the y register; value stored in

register is used during next phase)

With Regards to Claim 30, Chen discloses the method as recited in claim 24 wherein

the second number is implicitly identified in the single arithmetic instruction. (see Chen

col. 10, lines 32-36: rightmost k bits from multiplier are supplied back to the y register;

value stored in register is used during next phase)

With Regards to Claim 33, Chen discloses the method as recited in claim 18 wherein

the first and third numbers are specified in the single arithmetic instruction as first and

second source registers and a low order portion of the generated result is stored in a

destination location specified in the single arithmetic instruction. (see Chen col. 10,

lines 15-19: lower order k bits are supplied to adder to add two k bits addends at a time)

With Regards to Claim 34, Chen discloses the method as recited in claim 33 wherein

the partial result from an executed single arithmetic instruction is implicitly specified by

the single arithmetic instruction and wherein the second number is explicitly specified by

a third source register in the single arithmetic instruction. (see Chen col. 11, lines 34-

40: feedback; first using circuit; then using circuit again with register provided with

output from first operational stage; col. 10, lines 23-26: multiple-accumulate instruction;

first addend comes from the rightmost k bits of Z register; bits are added to the k bits in

the rightmost portion of the product A,B)

Bhushan discloses wherein a previously executed single arithmetic instruction. (see

Bhushan paragraph [0116], lines 14-20: instruction requires an operand, a result from a

previous instructions, the result may be bypassed under the direction of bypass routing

control)

It would have been obvious to one of ordinary skill in the art to modify Chen for a

previously executed single arithmetic instruction as taught by Bhushan. One of ordinary

skill in the art would have been motivated to employ the teachings of Bhushan in order

to provide an efficient method for an uncomplicated arithmetic circuit that is capable of

adding or subtracting numbers in redundant from and comparing a result without

requiring propagation of carry signals.   (see Bhushan paragraph [0062], lines 1-5)

With Regards to Claim 35, Chen discloses the method as recited in claim 33 wherein the partial result from an executed single arithmetic instruction is implicitly specified by the single arithmetic instruction and the second number is implicitly specified by the single arithmetic instruction. (see Chen col. 11, lines 34-40: feedback; first using circuit; then using circuit again with register provided with output from first operational stage; col. 10, lines 13-26: multiple-accumulate instruction; first addend comes from the rightmost k bits of Z register; bits are added to the k bits in the rightmost portion of the product A,B)

Bhushan discloses wherein a previously executed single arithmetic instruction. (see Bhushan paragraph [0116], lines 14-20: instruction requires an operand, a result from a previous instructions, the result may be bypassed under the direction of bypass routing control)

It would have been obvious to one of ordinary skill in the art to modify Chen for a previously executed single arithmetic instruction as taught by Bhushan. One of ordinary skill in the art would have been motivated to employ the teachings of Bhushan in order to provide an efficient method for an uncomplicated arithmetic circuit that is capable of adding or subtracting numbers in redundant from and comparing a result without requiring propagation of carry signals.   (see Bhushan paragraph [0062], lines 1-5)

With Regards to Claim 36, Chen discloses the method as recited in claim 23 further

comprising: in response to executing the subsequent single arithmetic instruction,

multiplying a fourth number and a fifth number, the fourth number being specified by the

subsequent single arithmetic instruction, adding implicitly the next partial multiplication

result and adding a sixth number to generate a second result, the second result

representing the fourth number multiplied by the fifth number summed with the next

partial result and the sixth number. (see Chen col. 11, lines 34-40: feedback; first using

circuit; then using circuit again with register provided with output from first operational

stage; col. 10, lines 13-26: multiple-accumulate instruction; first addend comes from the

rightmost k bits of Z register; bits are added to the k bits in the rightmost portion of the

product A,B)

With Regards to Claim 37, Chen discloses the method as recited in claim 36 wherein

the fifth number and the second number are equal.   (see Chen col. 6, lines 12-14;

distinct operands in pipelined mode (instructions))

With Regards to Claim 38, Chen discloses the method as recited in claim 36 further

comprising storing a high order portion of the second result to be implicitly added in

response to executing another subsequent single arithmetic instruction. (see Chen col.

11, lines 34-40: feedback; first using circuit; then using circuit again with register

provided with output from first operational stage; col. 10, lines 23-26: multiple-

accumulate instruction; first addend comes from the rightmost k bits of Z register; bits

are added to the k bits in the rightmost portion of the product A,B)

With Regards to Claim 39, Chen discloses the method as recited in claim 18 wherein

the first number is specified in the single arithmetic instruction in a first source register,

the second number is contained in a special register and is not specified in the single

arithmetic instruction, the third number is specified as a second source register in the

single arithmetic instruction and a low order portion of the generated result is stored in a

destination location specified in the single arithmetic instruction. (see Chen col. 6, lines

12-14; distinct operands in pipelined mode (instructions))

With Regards to Claim 40, Chen discloses the method as recited in claim 18 wherein

the first, second, and third numbers are specified by source operands in the single

arithmetic instruction. (see Chen col. 6, lines 12-14; distinct operands in pipelined mode

(instructions))

With Regards to Claim 41, Chen discloses the method as recited in claim 18 wherein a

destination location and one of the first number, the second number, and the third

number are specified by one operand in the single arithmetic instruction. (see Chen col.

6, lines 12-14; distinct operands in pipelined mode (instructions))

With Regards to Claim 42, Chen discloses the method as recited in claim 18 wherein

the multiplying and adding operations are implemented for binary polynomial fields.

(see Chen col. 4, lines 8-11: multiplication and addition are performed by large circuits;

col. 10, lines 13-36; col. 11, lines 34-40: multiplication with feedback; col. 6, lines 23-25:

arithmetic operations to support acceleration of cryptographic functions)

With Regards to Claim 43, Chen discloses a processor comprising an arithmetic

circuit, the processor configured to be responsive to execution of a single arithmetic

instruction to cause the arithmetic circuit to multiply a first number and a second number

and to add implicitly a high order portion of a partial result from an executed single

arithmetic instruction, thereby generating a result that represents the first number

multiplied by the second number summed with the high order portion of the partial

result; store at least a portion of the generated result; and use the stored at least a

portion of the generated result in a subsequent computation.   (see Chen col. 4, lines 8-

11: multiplication and addition are performed by large circuits; col. 10, lines 13-36; col.

11, lines 34-40: multiplication with feedback; col. 6, lines 23-25: arithmetic operations to

support acceleration of cryptographic functions)

Bhushan discloses wherein a result from a previously executed single arithmetic

instruction. (see Bhushan paragraph [0116], lines 14-20: instruction requires an

operand, a result from a previous instructions, the result may be bypassed under the

direction of bypass routing control)

It would have been obvious to one of ordinary skill in the art to modify Chen for a

result from a previously executed single arithmetic instruction as taught by Bhushan.

One of ordinary skill in the art would have been motivated to employ the teachings of

Bhushan in order to provide an efficient method for an uncomplicated arithmetic circuit

that is capable of adding or subtracting numbers in redundant from and comparing a result without requiring propagation of carry signals.   (see Bhushan paragraph [0062], lines 1-5)

With Regards to Claim 44, Chen discloses the processor as recited in claim 43, wherein to store at least a portion of the generated result, the processor is further responsive to the single arithmetic instruction to store a high order portion of the generated result into an extended carry register for use with execution of a subsequent single arithmetic instruction. (see Chen col. 11, lines 34-40: feedback; first using circuit; then using circuit again with register provided with output from first operational stage; col. 10, lines 23-26: multiple-accumulate instruction; first addend comes from the rightmost k bits of Z register; bits are added to the k bits in the rightmost portion of the product A,B)

With Regards to Claim 49, Chen discloses the processor as recited in claim 43 wherein the first and second numbers are specified in the single arithmetic instruction as first and second source registers. (see Chen col. 6, lines 12-14; distinct operands in pipelined mode (instructions))

With Regards to Claim 50, Chen discloses a processor comprising an arithmetic circuit, the processor configured to be responsive to execution of a single arithmetic instruction to; cause the arithmetic circuit to multiply a first number and a second

number to add a third number and to implicitly add a high order portion of a result from

an executed single arithmetic instruction thereby generating a result that represents the

first number multiplied with the second number, summed with the high order portion of

the previous result and with the third number; store at least a portion of the generated

result; and use the stored at least a portion of the generated result in a subsequent

computation. (see Chen col. 4, lines 8-11: multiplication and addition are performed by

large circuits; col. 10, lines 13-36; col. 11, lines 34-40: feedback; first using circuit; then

using circuit again with register provided with output from first operational stage

(multiplication with feedback); col. 6, lines 23-25: arithmetic operations to support

acceleration of cryptographic functions)

Bhushan discloses wherein a previous result from a previously executed single

arithmetic instruction. (see Bhushan paragraph [0116], lines 14-20: instruction requires

an operand, a result from a previous instructions, the result may be bypassed under the

direction of bypass routing control)

It would have been obvious to one of ordinary skill in the art to modify Chen for a

previous result from a previously executed single arithmetic instruction as taught by

Bhushan. One of ordinary skill in the art would have been motivated to employ the

teachings of Bhushan in order to provide an efficient method for an uncomplicated

arithmetic circuit that is capable of adding or subtracting numbers in redundant from and

comparing a result without requiring propagation of carry signals. (see Bhushan

paragraph [0062], lines 1-5)

With Regards to Claim 51, Chen discloses the processor as recited in claim 50

wherein to store at least a portion of the generated result, the processor is configured to

store a high order portion of the generated result for use with execution of a subsequent

single arithmetic instruction. (see Chen col. 11, lines 34-40: feedback; first using circuit;

then using circuit again with register provided with output from first operational stage;

col. 10, lines 23-26: multiple-accumulate instruction; first addend comes from the

rightmost k bits of Z register; bits are added to the k bits in the rightmost portion of the

product A,B)

With Regards to Claim 56, Chen discloses the processor as recited in claim 50,

wherein the first number is specified in the single arithmetic instruction as a first source

register, the second number is contained in a logically local register and is not specified

in the single arithmetic instruction, the third number is specified as a second source

register in the single arithmetic instruction and a low order portion of the result is stored

in a destination location specified in the single arithmetic instruction. (see Chen col. 6,

lines 12-14; distinct operands in pipelined mode (instructions); col. 10, lines 15-23: low

order k bits from multiplier are supplied to adder)

With Regards to Claim 57, Chen discloses a computer-readable storage medium,

comprising program instructions executable by a processor to implement a

cryptography application: wherein a single arithmetic instruction in the cryptography

application causes the processor to multiply a first number by a second number and to

implicitly add a high order portion of an executed single arithmetic instruction to

generate a result that represents the first number multiplied with the second number

and summed with the high order portion of an executed single arithmetic instruction,

wherein the single arithmetic instruction further causes the processor to store a high

order portion of the generated result for use with execution of a subsequent single

arithmetic instruction in the cryptography application. (see Chen col. 4, lines 8-11:

multiplication and addition are performed by large circuits; col. 10, lines 13-36; col. 11,

lines 34-40: multiplication with feedback; col. 6, lines 23-25: arithmetic operations to

support acceleration of cryptographic functions)

Bhushan discloses wherein a previously executed single arithmetic instruction to

generate a result. (see Bhushan paragraph [0116], lines 14-20: instruction requires an

operand, a result from a previous instructions, the result may be bypassed under the

direction of bypass routing control)

It would have been obvious to one of ordinary skill in the art to modify Chen for a

previously executed single arithmetic instruction to generate a result as taught by

Bhushan. One of ordinary skill in the art would have been motivated to employ the

teachings of Bhushan in order to provide an efficient method for an uncomplicated

arithmetic circuit that is capable of adding or subtracting numbers in redundant from and

comparing a result without requiring propagation of carry signals.   (see Bhushan

paragraph [0062], lines 1-5)

With Regards to Claim 58, Chen discloses the storage medium as recited in claim 57

wherein the single arithmetic instruction includes a first source operand and a second source operand, specifying the first number and the second number, and a destination operand wherein the single arithmetic instruction further causes the processor to store a low order portion of the generated result in a location specified by the destination operand. (see Chen col. 6, lines 12-14; distinct operands in pipelined mode (instructions); col. 10, lines 15-23: low order k bits from multiplier are supplied to adder)

With Regards to Claim 59, Chen discloses the storage medium as recited in claim 57, wherein the subsequent single arithmetic instruction causes the processor executing the subsequent single arithmetic instruction to multiply a third number by a fourth number and implicitly add the high order portion of the result. (see Chen col. 11, lines 34-40: feedback; first using circuit; then using circuit again with register provided with output from first operational stage; col. 10, lines 23-26: multiple-accumulate instruction; first addend comes from the rightmost k bits of Z register; bits are added to the k bits in the rightmost portion of the product A,B)

With Regards to Claim 60, Chen discloses the storage medium as recited in claim 59, wherein another single arithmetic instruction in the cryptography application causes the processor to multiply a fifth number by a sixth number and to generate another result without implicitly adding another high order portion of another executed result and to store a high order portion of the other result for use with another subsequent single arithmetic instruction. (see Chen col. 11, lines 34-40: feedback; first using circuit; then

using circuit again with register provided with output from first operational stage; col. 10,

lines 23-26: multiple-accumulate instruction; first addend comes from the rightmost k

bits of Z register; bits are added to the k bits in the rightmost portion of the product A,B)

Bhushan discloses wherein another previously executed result. (see Bhushan

paragraph [0116], lines 14-20: instruction requires an operand, a result from a previous

instructions, the result may be bypassed under the direction of bypass routing control)

It would have been obvious to one of ordinary skill in the art to modify Chen for

another previously executed result as taught by Bhushan. One of ordinary skill in the

art would have been motivated to employ the teachings of Bhushan in order to provide

an efficient method for an uncomplicated arithmetic circuit that is capable of adding or

subtracting numbers in redundant from and comparing a result without requiring

propagation of carry signals.   (see Bhushan paragraph [0062], lines 1-5)

With Regards to Claim 61, Chen discloses a computer-readable storage medium,

comprising program instructions executable by a processor to implement a

cryptography application: wherein a single arithmetic instruction in the cryptography

application causes the processor to: multiply a first number by a second number; add

implicitly a partial multiplication result from an executed single arithmetic instruction and

a third number to generate a result that represents the first number multiplied by the

second number summed with the partial multiplication result and summed with the third

number; and store a high order portion of the generated result for use with execution of

a subsequent single arithmetic instruction in the cryptography application. (see Chen

col. 4, lines 8-11: multiplication and addition are performed by large circuits; col. 10,

lines 13-36; col. 11, lines 34-40: feedback; first using circuit; then using circuit again

with register provided with output from first operational stage (multiplication with

feedback); col. 6, lines 23-25: arithmetic operations to support acceleration of

cryptographic functions; col. 3, lines 55-62: prior art implemented in software (computer

readable medium))

Bhushan discloses wherein a previously executed single arithmetic instruction. (see

Bhushan paragraph [0116], lines 14-20: instruction requires an operand, a result from a

previous instructions, the result may be bypassed under the direction of bypass routing

control)

It would have been obvious to one of ordinary skill in the art to modify Chen for a

previously executed single arithmetic instruction as taught by Bhushan. One of ordinary

skill in the art would have been motivated to employ the teachings of Bhushan in order

to provide an efficient method for an uncomplicated arithmetic circuit that is capable of

adding or subtracting numbers in redundant from and comparing a result without

requiring propagation of carry signals. (see Bhushan paragraph [0062], lines 1-5)

With Regards to Claim 62, Chen discloses the storage medium as recited in claim 61,

wherein the subsequent second single arithmetic instruction causes the processor to

multiply a fourth number by the second number to add a fifth number, and to implicitly

add the high order portion of the generated result. (see Chen col. 11, lines 34-40:

feedback; first using circuit; then using circuit again with register provided with output

from first operational stage; col. 10, lines 23-26: multiple-accumulate instruction; first

addend comes from the rightmost k bits of Z register; bits are added to the k bits in the

rightmost portion of the product A,B)

With Regards to Claim 63, Chen discloses the storage medium as recited in claim 61,

wherein the subsequent single arithmetic instruction causes the processor to multiply a

fourth number by a fifth number, to add a sixth number, and to implicitly add the high

order portion of the result. (see Chen col. 11, lines 34-40: feedback; first using circuit;

then using circuit again with register provided with output from first operational stage;

col. 10, lines 23-26: multiple-accumulate instruction; first addend comes from the

rightmost k bits of Z register; bits are added to the k bits in the rightmost portion of the

product A,B)

With Regards to Claim 64, Chen discloses a processor supporting a cryptography

application comprising: means, responsive to a single multiply-accumulate instruction in

the cryptography application, for multiplying a first number with a second number and

implicitly adding a partial result of an executed single multiply-accumulate instruction to

generate a result that represents the first number multiplied by the second number

summed with the partial result; and means for storing a high order portion of the result

for use with execution of a subsequent single multiply-accumulate instruction in the

cryptography application.   (see Chen col. 4, lines 8-11: multiplication and addition are

performed by large circuits; col. 10, lines 13-36; col. 11, lines 34-40: multiplication with

feedback; col. 6, lines 23-25: arithmetic operations to support acceleration of

cryptographic functions)

Bhushan discloses wherein a previously executed single arithmetic instruction. (see

Bhushan paragraph [0116], lines 14-20: instruction requires an operand, a result from a

previous instructions, the result may be bypassed under the direction of bypass routing

control)

It would have been obvious to one of ordinary skill in the art to modify Chen for a

previously executed single arithmetic instruction as taught by Bhushan. One of ordinary

skill in the art would have been motivated to employ the teachings of Bhushan in order

to provide an efficient method for an uncomplicated arithmetic circuit that is capable of

adding or subtracting numbers in redundant from and comparing a result without

requiring propagation of carry signals. (see Bhushan paragraph [0062], lines 1-5)

With Regards to Claim 65, Chen discloses a processor supporting a cryptography

application, comprising: means, responsive to a single multiply-accumulate instruction in

a cryptography application, for multiplying a first number with a second number, for

implicitly adding a partial result of an executed single multiply-accumulate instruction,

and for adding a third number to generate a result that represents the first number

multiplied by the second number summed with the partial result and the third number;

and means for storing a high order portion of the generated result for use with execution

of a subsequent multiply-accumulate instruction in the cryptography application. (see

Chen col. 4, lines 8-11: multiplication and addition are performed by large circuits; col.

10, lines 13-36; col. 11, lines 34-40: multiplication with feedback; col. 6, lines 23-25:

arithmetic operations to support acceleration of cryptographic functions)

Bhushan discloses wherein a previously executed single arithmetic instruction. (see

Bhushan paragraph [0116], lines 14-20: instruction requires an operand, a result from a

previous instructions, the result may be bypassed under the direction of bypass routing

control)

It would have been obvious to one of ordinary skill in the art to modify Chen for a

previously executed single arithmetic instruction as taught by Bhushan. One of ordinary

skill in the art would have been motivated to employ the teachings of Bhushan in order

to provide an efficient method for an uncomplicated arithmetic circuit that is capable of

adding or subtracting numbers in redundant from and comparing a result without

requiring propagation of carry signals. (see Bhushan paragraph [0062], lines 1-5)

6.   Claims **3, 20, 45, 52** are rejected under 35 U.S.C. 103(a) as being unpatentable

over **Chen-Bhushan** and further in view of **Lasher et al.** (US Patent No. **4,863,247**).

With Regards to Claim 3, Chen discloses the method as recited in claim 1, wherein the

partial result. (see Chen col. 10, lines 23-26: partial result; first rightmost k bits in Z

register; these bits are to the k bits in the rightmost portion of the product A,B) And,

Lasher discloses wherein the result is in redundant number representation. (see Lasher

col. 6, lines 6-9; col. 6, lines 16-18: redundant number representations)

It would have been obvious to one of ordinary skill in the art to modify Chen for a

result in redundant number representation as taught by Lasher.   One of ordinary skill in the art would have been motivated to employ the teachings of Lasher that fully parallel carry-free operation is provided for with reduced complexity.   (see Lasher col. 2, lines 57-62)

With Regards to Claim 20, Chen discloses the method as recited in claim 18, wherein the partial result. And, Lasher discloses wherein the result is in redundant number representation. (see Lasher col. 6, lines 6-9; col. 6, lines 16-18: redundant number representations)

It would have been obvious to one of ordinary skill in the art to modify Chen for a result in redundant number representation as taught by Lasher.   One of ordinary skill in the art would have been motivated to employ the teachings of Lasher in order that fully parallel carry-free operation is provided for with reduced complexity.   (see Lasher col. 2, lines 57-62)

With Regards to Claim 45, Chen discloses the processor as recited in claim 43 wherein the high order portion of the executed single arithmetic instruction is stored. And, Lasher discloses wherein the portion is stored in a redundant number representation. (see Lasher col. 6, lines 6-9; col. 6, lines 16-18: redundant number representations)

It would have been obvious to one of ordinary skill in the art to modify Chen for a result in redundant number representation as taught by Lasher.   One of ordinary skill in

the art would have been motivated to employ the teachings of Lasher in order that fully

parallel carry-free operation is provided for with reduced complexity.   (see Lasher col.

2, lines 57-62)

Bhushan discloses wherein the previously executed single arithmetic instruction. (see

Bhushan paragraph [0116], lines 14-20: instruction requires an operand, a result from a

previous instructions, the result may be bypassed under the direction of bypass routing

control)

It would have been obvious to one of ordinary skill in the art to modify Chen for the

previously executed single arithmetic instruction as taught by Bhushan. One of ordinary

skill in the art would have been motivated to employ the teachings of Bhushan in order

to provide an efficient method for an uncomplicated arithmetic circuit that is capable of

adding or subtracting numbers in redundant from and comparing a result without

requiring propagation of carry signals.   (see Bhushan paragraph [0062], lines 1-5)

With Regards to Claim 52, Chen discloses the processor as recited in claim 50

wherein the high order portion of the previous result is stored in a redundant number

representation. And, Lasher discloses wherein the portion is stored in redundant

number representation. (see Lasher col. 6, lines 6-9; col. 6, lines 16-18: redundant

number representations)

It would have been obvious to one of ordinary skill in the art to modify Chen for a

result in redundant number representation as taught by Lasher.   One of ordinary skill in

the art would have been motivated to employ the teachings of Lasher in order that fully

parallel carry-free operation is provided for with reduced complexity.   (see Lasher col.
2, lines 57-62)

7.   Claims **6 - 12, 24 - 29, 31, 32, 48, 53, 54, 55** are rejected under 35 U.S.C. 103(a)

as being unpatentable over **Chen-Bhushan** and further in view of **Stribaek et al.** (US

Patent No. **7,181,484**).

With Regards to Claim 6, Chen discloses the method as recited in claim 5, wherein

said storing the high order portion of the generated result comprises storing the high

order portion of the generated result into a register for use with execution of the

subsequent single arithmetic instruction. (see Chen col. 4, lines 8-11: multiplication and

addition are performed by large circuits; col. 10, lines 13-36; col. 11, lines 34-40:

multiplication with feedback; col. 6, lines 23-25: arithmetic operations to support

acceleration of cryptographic functions)   Chen does not specifically disclose an

extended carry register. And, Stribaek discloses wherein an extended carry register.

(see Stribaek col. 5, lines 41-45: load value extended carry operations)

It would have been obvious to one of ordinary skill in the art to modify Chen as

taught by Stribaek for usage of an extended carry register.   One of ordinary skill in the

art would have been motivated to employ the teachings of Stribaek to enable the

capability for extended precision in arithmetic calculations due to extensive and

increasing usage of public key cryptography.   (see Stribaek col. 1, lines 61-67)

With Regards to Claim 7, Chen discloses the method as recited in claim 6, further

comprising retrieving an indication of a current value of the register by executing

another single arithmetic instruction that multiplies a third number by a fourth number

and that implicitly adds current contents of the extended carry register to generate a

second result that represents the third number multiplied by the fourth number summed

with the current contents of the register. (see Chen col. 11, lines 34-40: feedback; first

using circuit; then using circuit again with register provided with output from first

operational stage; col. 10, lines 13-26: multiple-accumulate instruction; first addend

comes from the rightmost k bits of Z register; bits are added to the k bits in the rightmost

portion of the product A,B)   Chen does not specifically disclose an extended carry

register. And, Stribaek discloses wherein an extended carry register. (see Stribaek col.

5, lines 41-45: load value extended carry operations)

It would have been obvious to one of ordinary skill in the art to modify Chen as

taught by Stribaek for usage of an extended carry register.   One of ordinary skill in the

art would have been motivated to employ the teachings of Stribaek in order to enable

the capability for extended precision in arithmetic calculations due to extensive and

increasing usage of public key cryptography.   (see Stribaek col. 1, lines 61-67)

With Regards to Claim 8, Chen discloses the method as recited in claim 7, wherein a

low order portion of the second result contains the indication of the current value of the

register. (see Chen col. 6, lines 12-14; distinct operands in pipelined mode

(instructions); col. 10, lines 15-23: low order k bits from multiplier are supplied to adder)

Chen does not specifically disclose an extended carry register. And, Stribaek discloses

wherein an extended carry register. (see Stribaek col. 5, lines 41-45: load value

extended carry operations)

It would have been obvious to one of ordinary skill in the art to modify Chen as

taught by Stribaek for usage of an extended carry register. One of ordinary skill in the

art would have been motivated to employ the teachings of Stribaek in order to enable

the capability for extended precision in arithmetic calculations due to extensive and

increasing usage of public key cryptography. (see Stribaek col. 1, lines 61-67)

With Regards to Claim 9, Chen discloses the method as recited in claim 7, wherein the

third and fourth numbers are zero. (see Chen col. 6, lines 12-14; distinct operands in

pipelined mode (instructions))

With Regards to Claim 10, Chen discloses the method as recited in claim 6, further

comprising loading the register with a predetermined value by executing another single

arithmetic instruction that multiplies a third number by a fourth number and that implicitly

adds a current value of the extended carry register, to generate a result that represents

the third number multiplied by the fourth number summed with the current value of the

register, thereby loading the register with the predetermined value. (see Chen col. 11,

lines 34-40: feedback; first using circuit; then using circuit again with register provided

with output from first operational stage; col. 10, lines 13-26: multiple-accumulate

instruction; first addend comes from the rightmost k bits of Z register; bits are added to

the k bits in the rightmost portion of the product A,B) Chen does not specifically

disclose an extended carry register. And, Stribaek discloses wherein an extended carry

register. (see Stribaek col. 5, lines 41-45: load value extended carry operations)

It would have been obvious to one of ordinary skill in the art to modify Chen as

taught by Stribaek for usage of an extended carry register. One of ordinary skill in the

art would have been motivated to employ the teachings of Stribaek in order to enable

the capability for extended precision in arithmetic calculations due to extensive and

increasing usage of public key cryptography. (see Stribaek col. 1, lines 61-67)

With Regards to Claim 11, Stribaek discloses the method as recited in claim 6, further

comprising selecting one of a plurality of extended carry registers as the extended carry

register. (see Stribaek col. 5, lines 41-45: extended carry operations)

It would have been obvious to one of ordinary skill in the art to modify Chen as

taught by Stribaek for usage of an extended carry register. One of ordinary skill in the

art would have been motivated to employ the teachings of Stribaek in order to enable

the capability for extended precision in arithmetic calculations due to extensive and

increasing usage of public key cryptography. (see Stribaek col. 1, lines 61-67)

With Regards to Claim 12, Chen discloses the method as recited in claim 6, further

comprising accessing the register via at least one of a load instruction and a store

instruction. (see Chen col. 11, lines 48-51; col. 19, lines 7-10: load/store instruction)

Chen does not specifically disclose an extended carry register. And, Stribaek discloses

wherein an extended carry register. (see Stribaek col. 5, lines 41-45: extended carry operations)

It would have been obvious to one of ordinary skill in the art to modify Chen as taught by Stribaek for usage of an extended carry register. One of ordinary skill in the art would have been motivated to employ the teachings of Stribaek in order to enable the capability for extended precision in arithmetic calculations due to extensive and increasing usage of public key cryptography. (see Stribaek col. 1, lines 61-67)

With Regards to Claim 24, Chen discloses the method as recited in claim 23 wherein said storing the high order portion of the generated result comprises storing the high order portion of the generated result into a register for use with execution of the subsequent arithmetic instruction. (see Chen col. 11, lines 34-40: feedback; first using circuit; then using circuit again with register provided with output from first operational stage; col. 10, lines 13-26: multiple-accumulate instruction; first addend comes from the rightmost k bits of Z register; bits are added to the k bits in the rightmost portion of the product A,B) Chen does not specifically disclose an extended carry register. However, Stribaek discloses wherein an extended carry register. (see Stribaek col. 5, lines 41-45: extended carry operations)

It would have been obvious to one of ordinary skill in the art to modify Chen as taught by Stribaek to enable the capability for the usage of an extended carry register. One of ordinary skill in the art would have been motivated to employ the teachings of Stribaek in order to enable the capability for extended precision in arithmetic

calculations due to extensive and increasing usage of public key cryptography.   (see

Stribaek col. 1, lines 61-67)

With Regards to Claim 25, Chen discloses the method as recited in claim 24, further

comprising retrieving an indication of a current value of the register by executing

another single arithmetic instruction that multiplies a fourth number by a fifth number,

that implicitly adds current contents of the register, and that adds a sixth number to

generate a second result that represents the fourth number multiplied by the fifth

number summed with the current contents of the register and the sixth number. (see

Chen col. 11, lines 34-40: feedback; first using circuit; then using circuit again with

register provided with output from first operational stage; col. 10, lines 13-26: multiple-

accumulate instruction; first addend comes from the rightmost k bits of Z register; bits

are added to the k bits in the rightmost portion of the product A,B) Chen does not

specifically disclose an extended carry register. However, Stribaek discloses wherein

an extended carry register. (see Stribaek col. 5, lines 41-45: extended carry operations)

It would have been obvious to one of ordinary skill in the art to modify Chen as

taught by Stribaek for usage of an extended carry register.   One of ordinary skill in the

art would have been motivated to employ the teachings of Stribaek in order to enable

the capability for extended precision in arithmetic calculations due to extensive and

increasing usage of public key cryptography.   (see Stribaek col. 1, lines 61-67)

With Regards to Claim 26, Chen discloses the method as recited in claim 25, wherein

a low order portion of the second result contains the indication of the current value of

the register. (see Chen col. 6, lines 12-14; distinct operands in pipelined mode

(instructions); col. 10, lines 15-23: low order k bits from multiplier are supplied to adder)

Chen does not specifically disclose an extended carry register. However, Stribaek

discloses wherein an extended carry register. (see Stribaek col. 5, lines 41-45:

extended carry operations)

It would have been obvious to one of ordinary skill in the art to modify Chen as

taught by Stribaek for usage of an extended carry register.   One of ordinary skill in the

art would have been motivated to employ the teachings of Stribaek in order to enable

the capability for extended precision in arithmetic calculations due to extensive and

increasing usage of public key cryptography.   (see Stribaek col. 1, lines 61-67)

With Regards to Claim 27, Chen discloses the method as recited in claim 24, further

comprising loading the register with a predetermined value by executing another single

arithmetic instruction that multiplies a fourth number by a fifth number; and implicitly

adds a current value of the register and adds a sixth number, to generate a result that

represents the third number multiplied by the fourth number summed with the current

value of the register and summed with the sixth number and to store it in the register,

thereby loading the register with the predetermined value. (see Chen col. 11, lines 34-

40: feedback; first using circuit; then using circuit again with register provided with

output from first operational stage; col. 10, lines 13-26: multiple-accumulate instruction;

first addend comes from the rightmost k bits of Z register; bits are added to the k bits in

the rightmost portion of the product A,B)   Chen does not specifically disclose an

extended carry register. However, Stribaek discloses wherein an extended carry

register.   (see Stribaek col. 5, lines 41-45: extended carry operations)

It would have been obvious to one of ordinary skill in the art to modify Chen as

taught by Stribaek for usage of an extended carry register.   One of ordinary skill in the

art would have been motivated to employ the teachings of Stribaek in order to enable

the capability for extended precision in arithmetic calculations due to extensive and

increasing usage of public key cryptography.   (see Stribaek col. 1, lines 61-67)

With Regards to Claim 28, Stribaek discloses the method as recited in claim 24,

further comprising selecting one of a plurality of extended carry registers as the

extended carry register. (see Stribaek col. 5, lines 41-45: extended carry operations)

It would have been obvious to one of ordinary skill in the art to modify Chen as

taught by Stribaek for usage of an extended carry register.   One of ordinary skill in the

art would have been motivated to employ the teachings of Stribaek in order to enable

the capability for extended precision in arithmetic calculations due to extensive and

increasing usage of public key cryptography.   (see Stribaek col. 1, lines 61-67)

With Regards to Claim 29, Stribaek discloses the method as recited in claim 24,

further comprising accessing the extended carry register via at least one of a load

instruction and a store instruction. (see Stribaek col. 5, lines 41-45: extended carry

operations)

It would have been obvious to one of ordinary skill in the art to modify Chen as taught by Stribaek for usage of an extended carry register. One of ordinary skill in the art would have been motivated to employ the teachings of Stribaek in order to enable the capability for extended precision in arithmetic calculations due to extensive and increasing usage of public key cryptography. (see Stribaek col. 1, lines 61-67)

With Regards to Claim 31, Chen discloses the method as recited in claim 30 further comprising accessing a register storing the second number via at least one of a load instruction and a store instruction. (see Chen col. 11, lines 48-51; col. 19, lines 7-10: load/store instruction) Chen does not specifically disclose a special register. However, Stribaek discloses wherein a special register. (see Stribaek col. 5, lines 41-45: special register (extended carry register))

It would have been obvious to one of ordinary skill in the art to modify Chen as taught by Stribaek for usage of a special register (an extended carry register). One of ordinary skill in the art would have been motivated to employ the teachings of Stribaek in order to enable the capability for extended precision in arithmetic calculations due to extensive and increasing usage of public key cryptography. (see Stribaek col. 1, lines 61-67)

With Regards to Claim 32, Chen discloses the method as recited in claim 18 further comprising accessing a special register storing the second number via at least one of a load instruction and a store instruction. (see Chen col. 11, lines 48-51; col. 19, lines 7-

10: load/store instruction)   Chen does not specifically disclose a special register.

However, Stribaek discloses wherein a special register. (see Stribaek col. 5, lines 41-

45: extended carry operations; col. 7, lines 31-37; col. 9, lines 10-14: carry-save adder)

It would have been obvious to one of ordinary skill in the art to modify Chen as

taught by Stribaek for usage of a special register (an extended carry register).   One of

ordinary skill in the art would have been motivated to employ the teachings of Stribaek

in order to enable the capability for extended precision in arithmetic calculations due to

extensive and increasing usage of public key cryptography. (see Stribaek col. 1, lines

61-67)

With Regards to Claim 48, Stribaek discloses the processor as recited in claim 43,

wherein the extended carry register is a special register. (see Stribaek col. 5, lines 41-

45: extended carry register)

It would have been obvious to one of ordinary skill in the art to modify Chen as

taught by Stribaek for usage of a special register (an extended carry register).   One of

ordinary skill in the art would have been motivated to employ the teachings of Stribaek

in order to enable the capability for extended precision in arithmetic calculations due to

extensive and increasing usage of public key cryptography.   (see Stribaek col. 1, lines

61-67)

With Regards to Claim 53, Chen discloses the processor as recited in claim 50,

wherein the processor is configured to store the high order portion of the generated

result into a register. (see Chen col. 11, lines 34-40: feedback; first using circuit; then

using circuit again with register provided with output from first operational stage; col. 10,

lines 13-26: multiple-accumulate instruction; first addend comes from the rightmost k

bits of Z register; bits are added to the k bits in the rightmost portion of the product A,B)

Chen does not specifically disclose an extended carry register. However, Stribaek

discloses wherein an extended carry register. (see Stribaek col. 5, lines 41-45:

extended carry register)

It would have been obvious to one of ordinary skill in the art to modify Chen as

taught by Stribaek for usage of an extended carry register. One of ordinary skill in the

art would have been motivated to employ the teachings of Stribaek in order to enable

the capability for extended precision in arithmetic calculations due to extensive and

increasing usage of public key cryptography. (see Stribaek col. 1, lines 61-67)

With Regards to Claim 54, Chen discloses the processor as recited in claim 50,

wherein the register is a special register accessible by the processor via at least one of

load instruction and store instructions. (see Chen col. 11, lines 48-51; col. 19, lines 7-

10: load/store instruction) Chen does not specifically disclose an extended carry

register. However, Stribaek discloses wherein an extended carry register. (see

Stribaek col. 5, lines 41-45: extended carry register)

It would have been obvious to one of ordinary skill in the art to modify Chen as

taught by Stribaek for usage of an extended carry register. One of ordinary skill in the

art would have been motivated to employ the teachings of Stribaek in order to enable

the capability for extended precision in arithmetic calculations due to extensive and

increasing usage of public key cryptography.   (see Stribaek col. 1, lines 61-67)

With Regards to Claim 55, Chen discloses the processor as recited in claim 50,

wherein the register has an associated dirty bit indicating whether contents of the

register need to be saved on a context switch.   (see Chen col. 6, lines 12-14; distinct

operands in pipelined mode (instructions))   Chen does not specifically disclose an

extended carry register. However, Stribaek discloses wherein an extended carry

register. (see Stribaek col. 5, lines 41-45: extended carry register)

It would have been obvious to one of ordinary skill in the art to modify Chen as

taught by Stribaek for usage of an extended carry register.   One of ordinary skill in the

art would have been motivated to employ the teachings of Stribaek in order to enable

the capability for extended precision in arithmetic calculations due to extensive and

increasing usage of public key cryptography.   (see Stribaek col. 1, lines 61-67)

8.   Claim **17** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Chen-**

Bhushan and further in view of **Chen et al.** (US Patent No. **6,687,725**: referred to as

"Chen2").

With Regards to Claim 17, Chen discloses the method as recited in claim 1 wherein

the multiplying and adding are implemented. (see Chen col. 4, lines 8-11: multiplication

and addition are performed by large circuits; col. 10, lines 13-36; col. 11, lines 34-40:

multiplication with feedback; col. 6, lines 23-25: arithmetic operations to support

acceleration of cryptographic functions)   And, Chen2 discloses wherein to support XOR

operations for binary polynomial fields. (see Chen2 col. 4, line 64 - col. 5, line 2; col. 15,

lines 29-31: XOR operations)

It would have been obvious to one of ordinary skill in the art to modify Chen to

support XOR operations as taught by Chen2.   One of ordinary skill in the art would

have been motivated to employ the teachings of Chen2 to provide an arithmetic circuit

which can perform all arithmetic operations in the finite field, including addition,

multiplication, division, exponentiation and inverse multiplication.   (see Chen2 col. 3,

lines 17-21)

9.   Claims **46, 47** are rejected under 35 U.S.C. 103(a) as being unpatentable over

Chen-Bhushan-Lasher and further in view of **Stribaek**.

With Regards to Claim 46, Chen discloses the processor as recited in claim 45,

wherein the extended carry register is a register accessible via a processor instruction.

(see Chen col. 6, lines 12-14; distinct operands in pipelined mode (instructions)) Chen

does not specifically disclose an extended carry register. However, Stribaek discloses

wherein an extended carry register. (see Stribaek col. 5, lines 41-45: extended carry

operations)

It would have been obvious to one of ordinary skill in the art to modify Chen as

taught by Stribaek for usage of an extended carry register.   One of ordinary skill in the

art would have been motivated to employ the teachings of Stribaek in order to enable

the capability for extended precision in arithmetic calculations due to extensive and

increasing usage of public key cryptography.   (see Stribaek col. 1, lines 61-67)

With Regards to Claim 47, Chen discloses the processor as recited in claim 45,

wherein the register has an associated dirty bit indicating whether contents of the

register need to be saved on a context switch. (see Chen col. 6, lines 12-14; distinct

operands in pipelined mode (instructions)) Chen does not specifically disclose an

extended carry register. However, Stribaek discloses wherein an extended carry

register. (see Stribaek col. 5, lines 41-45: extended carry operations)

It would have been obvious to one of ordinary skill in the art to modify Chen as

taught by Stribaek for usage of an extended carry register.   One of ordinary skill in the

art would have been motivated to employ the teachings of Stribaek in order to enable

the capability for extended precision in arithmetic calculations due to extensive and

increasing usage of public key cryptography.   (see Stribaek col. 1, lines 61-67)

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Carlton V. Johnson whose telephone number is 571-

270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 -

5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone

number for the organization where this application or proceeding is assigned is 571-

273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business

Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO

Customer Service Representative or access to the automated information system, call

800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/David García Cervetti/
Primary Examiner, Art Unit 2436

Carlton V. Johnson
Examiner
Art Unit 2436

CVJ
June 8, 2009